DE1484

Amended Section of Page 2 Corresponding to the Last Paragraph

The procedure of the Fiat-Shamir scheme can be expounded as follows. A reliable system administrator selects a sufficiently large number n. Then, A prover selects his own private key a that is relatively prime with n, and calculates $b = a^2 \bmod n$. The prover discloses b. Then, the following protocol is repeated for a number of times:

(a) The prover selects a random integer ~~r ⊟ Z_n^*~~ $r \in Z_n^*$,where Z_n^* is a multiplicative group of order n, calculates $x = r^2$, and sends x to the verifier;

(b) The verifier selects a random number ~~⊟ ⊟ {0, 1}~~ $\varepsilon \in \{0, 1\}$, and sends ~~⊟~~ $\in$ to the prover;

(c) On receiving ~~⊟~~ ε, the prover calculates ~~$y = r$⊟$a^{⊟}$~~ $y = r \cdot a^{\varepsilon}$ mod n and sends y to the verifier; and

(d) The verifier examines whether ~~$y^2 = x$⊟$b^{⊟}$~~ $y^2 = x \cdot b^{\varepsilon}$ mod n is established. If true, then the verifier accepts the prover as a legitimate user and, otherwise, stops the protocol.

Amended Section of Page 3 Corresponding to the First Two Paragraphs

Various schemes have been developed based on the original Fiat-Schamir scheme, and follows the above-mentioned protocol.

On the other hand, the procedure of the Schnorr scheme is as follows. First, two primes numbers p and q are chosen, wherein q is a prime factor of p-1. Then, choose a not equal to 1, such that ~~a^q □ 1 (mod p)~~ $a^q \equiv 1$ (mod p). Then, a random number s, i.e., the private key, less than q is chosen. The public key $v = a^{-s}$ mod p is then calculated. Thereafter, the following protocol is executed:

(a) The prover selects a random number r less than q, and computes $x = a^r$ mod p, then sends x to the verifier;

(b) The verifier sends the prover a random number ~~□ □ Z_q^*~~ $\varepsilon \in Z_q^*$, where Z_q^* is a multiplicative group of order q;

(c) The prover computes ~~$y = r + s$□ mod q~~ $y = r + s\varepsilon \bmod q$ and sends y to the verifier; and

(d) The verifier verifies whether ~~$x = a^y$ □$v^{□}$~~ $x = a^y \cdot v^\varepsilon$ mod p is established. If true, then the verifier accepts the prover as a legitimate user and, otherwise, stops the protocol.

DE1484

Amended Section of Page 5 Corresponding to Line 2 and Line 18

~~□ Z_m^*~~ $\in Z_m^*$ to obtain a query R, storing the evidence (x, Q) and the

randomly selected number

selected number ~~ω □ Z_m^*~~ $\omega \in Z_m^*$ to obtain a query R, storing the evidence

(x, Q) and the

DE1484

Amended Section of Page 9 Corresponding to Line 10

Subsequently, the ~~prover~~ selects random numbers ~~r_1, r_2, r_3 □ Z_m^*~~ $r_1, r_2, r_3 \in Z_m^*$ and generates

DE1484

Amended Section of Page 10 Corresponding to Line 1

The verifier receives ~~the~~ evidence (x, Q), selects a randomly selected number

~~ω □~~ $\omega \in$